

Primjer konfiguracije PIX firewall-a: Interna (zaštićena) mreža – DMZ – Internet (“spoljni svijet”)

Sta treba da zadovolji konfiguracija koja će biti prikazana:

- Na DMZ interfejsu se nalazi Web server, Mail server i FTP server, kojima treba omogućiti pristup sa interneta. Pristup svim ostalim hostovima na unutrašnjoj mreži mora biti zabranjeno za korisnike koji pristupaju sa interneta.
Web server privatna adresa 10.1.1.5 – javna adresa 195.66.166.3
Mail server privatna adresa 10.1.1.10 – javna adresa 195.66.166.4
FTP server privatna adresa 10.1.1.15 – javna adresa 195.66.166.5
- Svim korisnicima na internoj mreži je dozvoljen neograničen pristup Internetu, kao i serverima na DMZ interfejsu
- Korisnicima sa Interneta nije dozvoljeno da pinguju uređaje u internoj mreži

Zakupljena je jedna C klasa adresa od ISP-a 195.66.166.*. Adrese .1 i .2 su predviđene za spoljasnji ruter, kao i za **outside** interfejs firewall-a. Adrese 3,4,5 su predviđene za unutrašnje servere kojima će korisnici sa interneta pristupati. Adrese od 6-14 su zauzete za servere koji su predviđeni za implementaciju u narednom periodu.

Izlaz komande **wr term** koja kada se otkuca, izlistava konfiguraciju koja je trenutno aktivna na PIX firewall-u. Boldovani text su linije konfiguracije koje nisu u okviru default konfiguracije. Iznad njih se nalazi objašnjenje šta koja od komanda (ili grupa komandi) predstavlja u našem primjeru konfiguracije.

```
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname vrsfirewall
domain-name noplance.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
no names
```

*!--- Kreiramo access listu sa imenom **serveri** koja dozvoljava da svi korisnici sa interneta mogu da pristupe javnim serverima na interfejsu DMZ*

```
access-list serveri permit tcp any host 195.66.166.3 eq http
access-list serveri permit tcp any host 195.66.166.4 eq smtp
access-list serveri permit tcp any host 195.66.166.5 eq ftp
!
pager lines 24
logging on
logging timestamp
no logging standby
logging console
logging monitor
logging queue 512
```

!--- Svi interfejsi su po default-u ugašeni. Definisanje IP adresa za interfejse, kao i način rada

```
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
ip address outside 195.66.166.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
ip address dmz 10.1.1.1 255.255.255.0
```

```
ip audit info action alarm
ip audit attack action alarm
arp timeout 14400
```

```
!--- Definisanje Address Translation (NAT) klase adresa koje će interni hostovi koristiti kada izlaze na internet
```

```
global (outside) 1 195.66.166.15-195.66.166.253
```

```
!--- Definisanje Port Address Translation (PAT) adrese koja će biti korištena kada se iskoriste sve adrese iz NAT klase
```

```
global (outside) 1 195.66.166.254
```

```
!--- Dozvoliti svim internim hostovima da koriste NAT ili PAT
```

```
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

```
!--- Definisanje statičke translacije za interni web server kojem će se pristupati sa Interneta
```

```
static (dmz,outside) 195.66.166.3 10.1.1.5 netmask 255.255.255.255 0 0
```

```
!--- Definisanje statičke translacije za interni mail server kojem će se pristupati sa Interneta
```

```
static (dmz,outside) 195.66.166.4 10.1.1.10 netmask 255.255.255.255 0 0
```

```
!--- Definisanje statičke translacije za interni ftp server kojem će se pristupati sa Interneta
```

```
static (dmz,outside) 195.66.166.5 10.1.1.15 netmask 255.255.255.255 0 0
```

```
!--- Ova staticka translacija onemogućava translaciju adresa kada se ide sa inside interfejsa na dmz interfejs
```

```
static (inside,dmz) 192.168.1.0 192.168.1.0 netmask 255.255.255.0
```

```
!
```

```
!--- Pridružiti access-listu serveri outside interfejsu
```

```
access-group serveri in interface outside
```

```
!
```

```
!--- Definisanje default rute ka ISP ruteru
```

```
route outside 0.0.0.0 0.0.0.0 195.66.166.1 1
```

```
!
```

```
timeout xlate 3:00:00
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
```

```
si
```

```
p 0:30:00 sip_media 0:02:00
```

```
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
```

!--- Dozvoliti hostu 192.168.1.100 da ostvari telnet konekciju na inside interfejs PIX-a

telnet 192.168.1.100 255.255.255.255 inside

```
snmp-server community public
no snmp-server enable traps
floodguard enable
terminal width 80
Cryptochecksum:d66eb04bc477f21ffbd5baa21ce0f85a
: end
!
!
```